REMARKS

Applicant respectfully requests consideration and allowance of the pending claims. Each of the independent claims 1, 27, 32, and 36 has been amended hereby. Several dependent claims are amended hereby to rectify minor informalities.

Claim Rejections Under § 102

Claims 1-8, 10-15, 27, 28 and 30-37 stand rejected as being unpatentable under 35 U.S.C. § 102(e) in view of U.S. Patent Publication No. 20030182574 to Whitten et al. ("Whitten"). Applicant respectfully traverses this rejection.

Amended independent claim 1 recites:

> An apparatus comprising:
> one or more processors;
> memory;
> *a media including game content that includes at least an executable file and a data file, the data file including content for use by the executable file during run-time execution of the executable file*; and
> a data protection portion including a file system alteration checking portion, stored in the memory and executable on one or more processors, that protects the apparatus from modification of the game content by determining whether the game content has been modified, wherein the data protection portion includes a file signature checking portion for checking whether a file signature of the data file is as expected for media that has not been modified, *the file signature checking portion being called during run-time execution of the executable file and after the executable file initiates access of the data file*, and
> if the game content has been modified, then the use of the data file within the apparatus fails. (Emphasis added.)

From claim 1, Whitten does not disclose "a media including game content that includes at least an executable file and a data file, the data file including

content for use by the executable file during run-time execution of the executable file;... the file signature checking portion being called during run-time execution of the executable file and after the executable file initiates access of the data file." Instead, Whitten discloses digital data (executable game code) that is first verified *before* it is executed completely to enable game play. To achieve verification, Whitten computes a digest for each section of the digital data. The computed digests are stored in an encrypted header digest. Before the digital data is executed to enable game play, the digital data sections are compared to the digests stored in the header digest to confirm that the digital data is valid. The header digest used by Whitten is not "content for use by the executable file during run-time execution," as in claim 1. Moreover, Whitten does not disclose a verification mechanism that is "called during run-time execution of the executable file and after the executable file initiates access of the data file," as is recited in claim 1.

More specifically, Whitten describes the use of a header associated with a game disc, where the header is used to validate the contents stored on the game disc *before* content on the game disc is executed. (*See paragraph [0056] of Whitten.*) The header contains a header digest that includes digest sections of the software that enables execution of a game. Each of these digest sections may correspond to digital data that is stored on the game disc. Before digital data is executed on the game disc, the plurality of the digest sections are compared with corresponding digital data stored on the game disc. (*See paragraph [0062] of Whitten.*) If any of the digest sections do not match corresponding digital data stored on the game disc, use of the game disc and the files thereon are prevented.

Whitten does not disclose that the described header digest is used for anything other than verifying the validity of digital data (i.e., executable code)

stored on the game disc. Certainly, Whitten does not disclose that the header digest is a "data file including content for use by the executable file during run-time execution of the executable file," as is set forth in claim 1. For at least this reason, the rejection of claim 1 should be withdrawn.

Additionally, the Whitten system validates all data stored on a game disc before a file thereon is executed to enable normal run-time use. Whitten explicitly states in paragraph [0064] that the validation policies must be finished *before* the digital data may complete execution and begin normal run-time operation. In distinction, an implementation according to the instant Application is capable of verifying data "during run-time execution of the executable file and after the executable file initiates access of the data file," as is recited in claim 1. Therefore, at least one implementation according to the instant Application verifies data as access thereto is required. For at least this additional reason, the rejection of claim 1 should be withdrawn.

For at least the reasons stated above, Applicant respectfully requests the Office to reconsider and withdraw the rejection of claim 1.

Dependent claims 2-7 and 10-15 depend from claim 1. The rejection with regard to these claims should be withdrawn by virtue of the dependency. Moreover, these claims recite features that, when taken together with those of claim 1, are not disclosed by Whitten.

Dependent claim 8 has been canceled without prejudice. According, Applicant respectfully submits that the rejection thereof is now moot. Applicant respectfully requests the Office to reconsider and withdraw the rejection of claim 8.

Amended independent claim 27 recites:

> A method comprising:
>
> providing a media comprising media content, wherein the media content comprises game content, which includes at least *an executable file and a data file, the data file including content for use by the executable file during run-time execution of the executable file*;
>
> examining the data file for modifications, the examining comprising:
>
> *comparing an actual signature of the data file with an expected signature of the data file, the comparing initiated during run-time execution of the executable file and after the executable file initiates access of the data file*; and
>
> enabling access to the data file based on the examining. (Emphasis added.)

From claim 27, Whitten does not disclose "an executable file and a data file, the data file including content for use by the executable file during run-time execution of the executable file;... comparing an actual signature of the data file with an expected signature of the data file, the comparing initiated during run-time execution of the executable file and after the executable file initiates access of the data file." Instead, Whitten discloses digital data (executable game code) that is first verified *before* it is executed completely to enable game play. To achieve verification, Whitten computes a digest for each section of the digital data. The computed digests are stored in an encrypted header digest. Before the digital data is executed to enable game play, the digital data sections are compared to the digests stored in the header digest to confirm that the digital data is valid. The header digest used by Whitten is not "content for use by the executable file during run-time execution," as in claim 27. Moreover, Whitten does not disclose a comparing mechanism that is initiated "during run-time execution of the

executable file and after the executable file initiates access of the data file," as is recited in claim 27.

Additional details concerning the deficiencies of Whitten are given hereinabove, and such discussion may be applied to claim 27, as well. The Office is respectfully requested to consider the above discussion.

For at least the reasons stated above, Applicant respectfully requests the Office to reconsider and withdraw the rejection of claim 27.

Dependent claims 28, 30 and 31 depend from claim 27. The rejection with regard to these claims should be withdrawn by virtue of the dependency. Moreover, these claims recite features that are not disclosed by Whitten.

Amended independent claim 32 recites:

> A computer storage media comprising computer-readable instructions for implementing the computerized method of:
>
> *verifying whether a provided media comprising media content conforms to a stored media type definition, the media content including content for use by an executable file during run-time execution of the executable file*;
>
> examining the media content for alterations in format and content of files within the media content based on an actual and an expected signature of the media content, *the examining initiated during run-time execution of the executable file and after the executable file initiates access of the media content*; and
>
> accessing the media content of the provided media if the provided media conforms to the stored media type definition and if the actual signature of the content matches the expected signature of the content. (Emphasis added.)

From claim 32, Whitten does not disclose "verifying whether a provided media comprising media content conforms to a stored media type definition, the media content including content for use by an executable file during run-time execution of the executable file;... examining the media content for alterations in format and content of files within the media content based on an actual and an

expected signature of the media content, the examining initiated during run-time execution of the executable file and after the executable file initiates access of the media content." Instead, Whitten discloses digital data (executable game code) that is first verified *before* it is executed completely to enable game play. To achieve verification, Whitten computes a digest for each section of the digital data. The computed digests are stored in an encrypted header digest. Before the digital data is executed to enable game play, the digital data sections are compared to the digests stored in the header digest to confirm that the digital data is valid. The header digest used by Whitten is not "content for use by an executable file during run-time execution of the executable file," as in claim 32. Moreover, Whitten does not disclose an examination mechanism that is "initiated during run-time execution of the executable file and after the executable file initiates access of the media content," as is recited in claim 32.

Additional details concerning the deficiencies of Whitten are give hereinabove, and such discussion may be applied to claim 32, as well. The Office is respectfully requested to consider the above discussion.

For at least the reasons stated above, Applicant respectfully requests the Office to reconsider and withdraw the rejection of claim 32.

Dependent claim 33 depends from claim 32. The rejection with regard to this claim should be withdrawn by virtue of the dependency. Moreover, this claim 33 recites features that are not disclosed by Whitten.

Independent claim 34 and dependent claim 35 have been canceled hereby without prejudice. According Applicant respectfully submits that the rejection thereof is now moot. Applicant respectfully requests the Office to reconsider and withdraw the rejection of claims 34 and 35.

Amended independent claim 36 recites:

> A computer storage media comprising computer-readable instruction for implementing the computerized method of:
>
> verifying authenticity of a provided media based on media type definition stored in game console executable files in the provided media;
>
> matching actual signatures of the game console executable files with expected signatures of the game console executable files if the authenticity of the provided media is verified;
>
> executing the game console executable files if the actual signatures match the expected signatures;
>
> *requesting game content data files to be loaded by the game console executable files and during run-time execution thereof, the game content data files including content for use by the game console executable files*;
>
> comparing actual signatures of the game content data files with expected signatures of the game content data files before the game content data files are loaded; and
>
> launching game content on the provided media if the actual signatures of the game content data files match the expected signatures of the game content data files. (Emphasis added.)

From claim 36, Whitten does not disclose "requesting game content data files to be loaded by the game console executable files and during run-time execution thereof, the game content data files including content for use by the game console executable files." Instead, Whitten discloses digital data (executable game code) that is first verified *before* it is executed completely to enable game play. To achieve verification, Whitten computes a digest for each section of the digital data. The computed digests are stored in an encrypted header digest. Before the digital data is executed to enable game play, the digital data sections are compared to the digests stored in the header digest to confirm that the digital data is valid. Therefore, Whitten does not disclose "requesting game content data files to be loaded by the game console executable files and during run-time

execution thereof, the game content data files including content for use by the game console executable files," as is recited in claim 36.

Additional details concerning the deficiencies of Whitten are given hereinabove, and such discussion may be applied to claim 36, as well. The Office is respectfully requested to consider the above discussion.

For at least the reasons stated above, Applicant respectfully requests the Office to reconsider and withdraw the rejection of claim 36.

Dependent claim 37 depends from claim 36. The rejection with regard to this claim should be withdrawn by virtue of the dependency. Moreover, this claim 37 recites features that are not disclosed by Whitten.

Conclusion

In accordance with the foregoing remarks, Applicant believes that the pending claims are allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney at the provided email address.

Respectfully Submitted,

Dated: February 4, 2008

By: /Tim R. Wyckoff, Reg. No. 46,175/
David S. Lee
Reg. No. 38,222
By
Tim R. Wyckoff
Reg. No. 46,175
Email: wyc_law@live.com